DIGITAL FAIRNESS ACT

EXECUTIVE SUMMARY

Overall, FEDMA agrees that the exploitation of consumers' vulnerabilities to personalise commercial offers is an unacceptable practice. However, it is our belief that existing laws already enable to address this situation. Adding a new layer of rules on this topic would complexify further the legal framework, undermine the functioning of the single market and make it more difficult for European start-ups and SMEs to flourish.

I. **Unfair consumer practices & consumer choice** | **Key message**: As the Commission is exploring whether consumers could express their preferences regarding personalised advertising through a simple and effective (i.e. centralised) opt-in or opt-out system, FEDMA recalls ongoing challenges with the ePrivacy Directive, GDPR consent requirements, and competition implications.

II. **Unfair consumer practices & vulnerable consumers** | **Key message**: Rather than adding new rules, FEDMA recommends leveraging existing legislations, in particular the UCPD's provision on 'undue influence', the DSA's ban on personalised ads based on sensitive data, and the GDPR's risk-based approach.

III. **Dark patterns** | **Key message**: Rather than adding new rules, FEDMA recommends issuing additional guidelines, including the missing DSA guidelines on dark patterns.

IV. **Digital contracts & subscriptions**| **Key message**: Rather than adding new rules, FEDMA recommends assessing the future transposition and implementation of the Directive on the marketing of financial services at a distance (DMFSD) and its cross-sectoral requirement for a withdrawal function for all online contracts.

V. **Simplification measures** | **Key message:** Any possible legislative change should contribute to enhanced consumer protection and simplification of the regulatory environment for Small and Medium Enterprises (SMEs).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

I. Unfair personalisation practices & consumer choice

FEDMA would like to express concerns regarding the potential introduction of a simple and effective way for consumers to refuse or consent to personalised advertising, whether in the form of a general opt-out or opt-in system. Such a measure, which echoes similar centralized consumer choice ideas already (unsuccessfully) explored in the withdrawn ePrivacy Regulation proposal and the Cookie Pledge initiative, raises serious legal, practical, and market-related questions that warrant a more careful and comprehensive assessment.

1. Legal conflicts with the current framework: ePrivacy and GDPR

A key challenge with centralising user choices is the incompatibility with the current legal framework, notably Article 5(3) of the ePrivacy Directive. Most forms of digital advertising, whether personalised or contextual, require access to or storage of information in the user's terminal equipment, and thus fall under the scope of this provision, which mandates prior user consent.

The EDPB's draft Guidelines 02/2023 further expand the interpretation of Article 5(3), potentially triggering consent for a broader range of interactions. In practice, this could result in more frequent consent prompts, worsening the issue of *consent fatigue*, which the proposed centralisation is intended to mitigate.

While the GDPR's granular and specific consent requirements remain a critical obstacle to the design of any centralised system, the EDPB has acknowledged that software settings could be used to allow users to express their choice to refuse access or storage via such settings. However, this would require a paradigm shift away from the current consent-based regime under the ePrivacy Directive.

2. Need for Legal Reform to Enable Risk-Based Approaches

FEDMA has carried out an analysis showing that a long-term solution may require repealing the ePrivacy Directive and governing access/storage operations under the GDPR and the forthcoming Digital Networks Act. This would allow for a more coherent and risk-based framework, in which digital advertising could rely on alternative legal bases to consent depending on the risk level of the processing activity.

This approach would align with ongoing regulatory developments in other jurisdictions. For instance, the UK Information Commissioner's Office (ICO) is currently exploring a risk-based framework for certain advertising use cases that pose a low risk to users' privacy. The goal is to unlock innovation and support business growth, while ensuring user protection and enhancing the user experience.

3. Risks of Market Distortion and Undermining Media Sustainability

Centralising advertising preferences through software-level settings (e.g. browsers or OS-level interfaces) risks reinforcing the dominance of large digital platforms that already control significant parts of the online environment and can collect user data independently of third-party tracking technologies.

This could have a negative impact on competition, disproportionately affecting independent publishers and SMEs who rely on responsible and privacy-compliant advertising models to fund

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

free content and services. This also echoed by the recent decision by the French Competition Authority regarding the illegality of Apple ATT. As such, any centralization also undermines the objectives of the Digital Markets Act (DMA), which aims to foster fair and open digital markets by preventing entrenched gatekeeper positions.

Importantly, while centralised tools for users' choices could be considered in the future, they should never override publishers' freedom to choose their business model, their capacity to engage directly with their audience, or the users' ability to make choices directly with publishers. Any new solution must safeguard this critical relationship and allow for contextual, publisher-level interactions.

4. Timing and the Need for Evidence-Based Policy

Before proposing any new rules on personalised advertising, it is essential that the Commission conduct a thorough assessment of the effectiveness and real-world impact of existing legislation, notably the Digital Services Act (DSA).

DSA rules on advertising transparency and profiling have only started applying to all platforms as of February 2024. Drawing regulatory conclusions before allowing these provisions to take effect and be properly evaluated would be premature.

Moreover, the Commission should consider the findings of its ongoing stakeholder consultations, such as the DSA workshops on a possible advertising Code of Conduct, and the results of the study led by AWO on how the DSA and DMA are impacting the advertising ecosystem. These initiatives will offer valuable insight into existing industry practices, implementation challenges, and possible areas for improvement, insights that should inform any future policy action.

In sum, we encourage the Commission to take a measured, evidence-based approach and explore future-proof alternatives such as risk-based models, enhanced user transparency, and frameworks that support both consumer rights and a competitive, diverse digital advertising ecosystem.

II. Unfair personalisation practices & vulnerable consumers

As the European Commission is considering additional rules on personalized advertising to mitigate risks of exploiting, intentionally or negligently, consumers' vulnerabilities, one should carefully assess the interplay between existing legal frameworks and new potential regulatory measures.

1. Untapped potential of Article 8 UCPD

First, FEDMA believes that the principle of "undue influence" in Article 8 UCPD already provides a legal basis to address manipulative personalization tactics, particularly when traders exploit specific vulnerabilities to influence consumer decisions. This provision already offers a flexible legal basis that could be enforced more effectively with the right interpretative support. However, the Commission appears hesitant to rely on this clause, citing concerns over legal certainty due to a lack of case law, limited national experience with the concept of aggression, and the non-

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

binding nature of EU guidance. Yet, these are not valid reasons to dismiss the legal potential of Article 8.

First, the lack of case law should prompt the Commission to promote the use of this provision and to clarify its application, rather than seek to legislate anew. Second, EU guidance already acknowledges that the use of consumer vulnerabilities for commercial gain may constitute undue influence. If this is not sufficiently clear to Member States, the Commission should strengthen its guidance, not sideline it. Third, unfamiliarity with the concept of aggression highlights the need for capacity-building and coordinated enforcement, which EU-level guidance is designed to support. It is almost contradictory that the Fitness Check simultaneously stresses the need for more legal certainty on how existing UCPD principles apply to new digital practices, while pointing to the non-binding nature of the very guidelines created to provide that certainty, as a limitation. Rather than developing entirely new legal instruments, the Commission should invest in unlocking the full potential of the UCPD's existing provisions and reinforce their practical implementation through clearer and more authoritative guidance.

2. Leveraging GDPR to address vulnerability

Additionally, Article 9 GDPR already restricts the processing of sensitive personal data, which could include information about an individual's mental health, age, or socio-economic status, key indicators of vulnerability. This restriction is further reinforced through the ban on targeted advertising using sensitive data and minors' data in the DSA whose effectiveness still needs to be evaluated. However, the Commission's Fitness Check points out that it is unclear whether Article 9 GPDR on sensitive data covers all types of vulnerabilities that could be broadly considered as sensitive in the B2C context. We therefore underline that the GDPR already offers relevant protections against the exploitation of vulnerable individuals beyond Article 9. Recital 75 GDPR recognizes the risks of processing that may result in discrimination or harm, particularly where data subjects are vulnerable. The fairness principle (Article 5(1)(a)) requires considering how the data processing affects the interests of the people concerned, as a group and individually, which implicitly discourages exploitative profiling. Additionally, Data Protection Impact Assessments (DPIAs) are mandatory where processing is likely to result in high risks, including when vulnerabilities are involved.

For example, if a company were to infer an individual's emotional vulnerability due to the loss of a family member through online searches (e.g., for funeral services or grief counselling) and use this information to target marketing for products like expensive memorial services or high-interest personal loans, such processing would raise serious compliance concerns under the GDPR. Even if the data does not formally fall under Article 9's special categories, the GDPR's fairness principle (Article 5(1)(a)) and transparency requirements (Articles 12–14) would still apply. In this case, leveraging emotional distress without the individual's informed and freely given consent (Article 6 and Recital 42 GDPR) would likely be deemed unfair and unlawful profiling. A DPIA under Article 35 would also likely be required given the heightened risks to the individual's rights and freedoms. The Commission's own Fitness Check acknowledges that the intersection between consumer protection and data protection law requires further assessment,

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

highlighting that the tools to address these concerns already exist, and that better integration and enforcement could be prioritized over blanket bans.

3. Call for GDPR guidance on profiling individuals in vulnerable circumstances

To ensure greater legal clarity and consistency in the application of the GDPR to personalized marketing practices that may exploit consumer vulnerabilities, the European Commission should develop, along with the European Data Protection Board (EDPB) and national consumer protection authorities when relevant, guidance to clarify:

- How GDPR provisions, particularly the fairness principle (Article 5(1)(a)), purpose limitation (Article 5(1)(b)), data minimization (Article 5(1)(c)), and Article 9 on special categories of data, apply to the profiling of vulnerable individuals.
- Which types of inferred vulnerability (e.g., emotional distress, socio-economic hardship, cognitive limitations) may trigger heightened data protection requirements.
- How the obligation to conduct Data Protection Impact Assessments (Article 35) applies to high-risk processing involving vulnerability-based targeting.
- How existing GDPR rights (e.g., access, objection, restriction) can be leveraged by consumers to challenge or limit such profiling.

This initiative would:

- Promote greater legal certainty for businesses and enforcement authorities;
- Avoid premature or overlapping rules under the Digital Fairness Act;
- Support a coherent and proportionate approach to protecting vulnerable consumers in the digital environment, fully leveraging the existing GDPR framework.

4. Challenges of defining and detecting vulnerability

Should the Commission conclude that the current legal framework is inadequate, the implementation of an additional rules on personalized advertising and vulnerable consumers would nevertheless raise important issues. A key challenge would be the practical difficulty for businesses in identifying whether a consumer is vulnerable. Without clear indicators, companies may face a dilemma: either collect more personal (and potentially sensitive) data to assess vulnerability, thereby increasing the risk of non-compliance with the GDPR, or avoid collecting such data and risk unknowingly targeting a vulnerable person, thus breaching the DFA. To navigate this, the Commission might be tempted to propose a “reasonable degree of certainty” threshold, similar to the wording used in Article 28(2) DSA regarding advertising to minors. However, such vague standards only create legal uncertainty, undermining one of the DFA’s core goals. Should the Commission nonetheless pursue this route, the legal provision should be supported by concrete criteria or contextual indicators to help businesses act responsibly without overstepping GDPR limits. These would likely include sector-specific red flags (e.g. gambling, high-interest loans, weight-loss products), behavioral signals (e.g. browsing patterns indicating distress), or situational contexts (e.g. time of day, language suggesting urgency or distress).

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

However, even this approach has its limitations. Nowadays, many companies in the advertising ecosystem already implement safeguards, such as refusing to provide marketing and advertising services for products in high-risk sectors like gambling or payday loans, or strict due diligence procedures when deciding to work with a new client. However, faced with increasing regulatory uncertainty and the difficulty of assessing vulnerability without explicit data, more companies may opt to withdraw from serving a growing number of legitimate sectors, potentially stifling competition and consumer access to lawful products.

5. Toward a more balanced and effective approach

Finally, any new rule should account for the dynamic and contextual nature of vulnerability. Individuals may experience temporary vulnerability due to changing life circumstances, which businesses cannot and should not attempt to monitor through intrusive data collection. A more effective approach lies in ex post safeguards that empower consumers, particularly vulnerable ones, to retain meaningful control over their data. These include robust opt-out mechanisms, clear and simple information on data use and rights, easily accessible channels for complaints, and transparent ways to access one's data. These measures, grounded in GDPR principles, offer a more balanced, consumer-centric model for responsible personalization without the overreach or legal ambiguity of a one-size-fits-all ban.

III. Dark patterns

1. Prioritising existing legal tools before introducing new rules

As part of its efforts to regulate additional forms of dark patterns through the DFA, the European Commission should first ensure that the tools already available under existing legislation are fully explored and clarified. Notably, the Commission has yet to issue guidance on the application of Article 25 DSA, which directly prohibits the use of deceptive or manipulative online interfaces by online platforms. The practices listed under Article 25(3) DSA significantly overlap with those identified in the Fitness Check. Providing guidance on Article 25 DSA, even if non-binding, would be an important step in enhancing legal certainty and encouraging compliance across the digital ecosystem. This guidance should then be followed by a formal evaluation of effectiveness of the DSA. In parallel, it would also be coherent to clarify the application of the UCPD to dark patterns through updated guidance as the UCPD makes it possible to penalize unfair commercial practices even if they are not included in a list. This would help make the risks for users more foreseeable and create a fairer competitive environment among traders. If, over time, this approach proves insufficient, a more stringent step could be considered, such as carefully integrating specific, harmful practices into Annex I of the UCPD to strengthen legal certainty.

2. Risks of a general 'fairness by design' duty

In this context, the proposal to introduce a general "fairness by design" duty raises several concerns. While the intention to embed consumer protection considerations into the product development lifecycle is welcome, such a duty would risk creating a high degree of legal uncertainty. A comparable obligation under Article 25 GDPR (data protection by design and by default) has already sparked considerable interpretation challenges, despite guidance from the

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org

European Data Protection Board (EDPB). Without clear boundaries or definitions, the same risk applies to the proposed fairness duty. Moreover, the necessity of this provision is questionable, as it would arguably add limited value beyond the general fairness clause under Article 5(2) UCPD. If the legislator proceeds with introducing such a principle, it is crucial that detailed guidance is provided to ensure (1) workable, realistic standards that traders can operationalise, and (2) a clear articulation of how this new duty would interact with the fairness principle under the GDPR, in order to ensure legal coherence and avoid duplication.

IV. Issues with digital contracts & subscriptions

1. The role of digital subscriptions in consumer engagement and innovation

Digital subscriptions play a central role in the modern customer engagement framework and are a cornerstone of data-driven marketing. They enable traders to build long-term relationships with consumers, offering ongoing access to products, services, or content tailored to their preferences. In return, subscriptions provide valuable insights into consumer behaviour, allowing for more relevant and personalised marketing, improved user experience, and greater brand loyalty. As such, they contribute to the digital economy's efficiency and innovation. However, their success depends on maintaining consumer trust, including through clear and fair cancellation mechanisms that respect user autonomy without undermining legitimate business models.

2. Upcoming new rules can already address cancellation concerns

In this regard, the recent revision and repeal of the Directive on the marketing of financial services at a distance (DMFSD) already introduces specific measures to address the very concerns cited by the Commission. Article 11a requires traders to provide a prominent, easily accessible withdrawal function, such as a cancellation button, for all distance contracts concluded through online interfaces. Traders must also acknowledge receipt of the withdrawal on a durable medium, thereby ensuring consumers can easily understand whether their cancellation request was successful. These provisions directly respond to the technical and interface-related challenges identified by the Commission. Given that EU Member States are only required to transpose these provisions by December 2025 and apply them from June 2026, it would be premature to introduce a new layer of rules through the Digital Fairness Act. Doing so would risk unnecessary regulatory duplication and add complexity for businesses, contradicting the Commission's stated aim to address only genuine regulatory gaps and ensure a coherent legal framework for consumer protection in the digital age.

V. Simplification measures

Any possible legislative change proposed in any of the areas above should contribute to enhanced consumer protection and simplification of the regulatory environment. In addition, the Digital Fairness Act could also address other issues with a view to further reducing compliance costs while improving effective consumer protection. The Digital Fairness Fitness Check has identified potential for targeted simplification and burden reduction for traders, specifically in the area of information requirements and the right of withdrawal.

Federation of European Data and Marketing
Rue de la Loi 155, 1040 Brussels
+32 2 779 4268 www.fedma.org